Third-party verifiable voting systems: addressing motivation and incentives in e-voting

Robbie Simpson, Tim Storer

University of Glasgow, Glasgow, G12 8QQ

Abstract

Voter-verifiable voting systems place significant demands of both effort and knowledge onto ordinary voters who have only limited incentives to participate. We suggest the use of third-party verifiable voting systems, harnessing the very strong incentives for candidates and observers to verify that votes are correctly counted. A generic modification enabling this via the use of pre-filled ballots and secure depositing is outlined and we demonstrate this modification by applying it to two major voter-verifiable voting systems. Additionally, potential vulnerabilities of this approach are discussed.

1. Introduction

Receipt-free, voter-verifiable voting systems are the current gold standard in electronic voting system research, with numerous authors having proposed a plethora of schemes, including Scantegrity [1, 2]; ThreeBallot [3]; Scratch and vote [4, 5]; Chaum's visual cryptography scheme [6]; Prêt à Voter [7, 8]; Randell and Ryan's scheme modelled on fruit machines [9]; Reynolds's scheme [10] and voter verified secured paper audit trails [11].

A Receipt-free voter-verifiable (RFVV) scheme enables a voter to obtain assurances that the election has been operated fairly and that their vote has been counted, without the unfortunate side-effect of revealing the voter's choice to anyone else (and violating voting privacy, a requirement in many democratic jurisdictions). This property mitigates the perceived difficulty of verifying the machinery of an election directly (as is done in paper-based elections) due to the complexity and opacity of computer-based technology. As a consequence, elections can leverage the greater efficiency and accuracy of computer based elections, without compromising on the integrity or transparency of the result. An important characteristic of receipt-free voting is that voters themselves must not be able to prove how they voted; this prevents voters from being coerced or bribed.

In a typical RFVV scheme, a voter interacts with the voting system in a secure, isolated environment, such as a polling booth, to vote and also construct a *witness* for their vote. The witness is a document that provides the voter with some assurance that their vote has been counted correctly (that the voting system has committed to the value of their vote and cannot change it without detection). Most commonly this witness is constructed using cryptographic methods that allow some information about the vote to be recorded, without revealing the particular candidate or option voted for. As a result, the voter cannot use their witness to prove how they voted.

The voter must submit their vote to the voting system, just as in a paper based election. However, unlike the vote, the voter may remove the witness from the polling station and use it later to audit information published about the election by the voting system. If the witness shows that the voter's choice has not been correctly counted the voter may be able to have the

result overturned or corrected. Crucially, the witness only provides sufficient information for the voter to confirm that their vote has been correctly counted: it does not provide sufficient information for a third party to reconstruct *how* the voter voted.

A necessary consequence of the use of a RFVV scheme for an election is that responsibility for assuring an election result is placed on the voters in the election. This is significant: the design of voting schemes is often treated as a purely technical or even theoretical problem, in which the various actors are treated as neutral agents or software processes. However, voting schemes are implemented as socio-technical voting systems, involving a range of organisations and actors all with their own expectations, incentives and capabilities. These factors can impose significant constraints on the design of a voting scheme.

By contrast, the design of all RFVV schemes makes several implicit assumptions about the majority of voters who participate in real elections:

- That voters understand the general purpose of the verification method and the information provided (and not provided) by the witness.
- That voters can perform the witness construction process correctly and determine if their witness is an accurate encoding of their vote.
- That voters are able to correctly operate the vote verification mechanism and can distinguish between a correctly and incorrectly counted vote.
- That voters are motivated to perform the verification of their vote using the witness.
- That voters are able and willing to invoke dispute resolution procedures if they believe their witness is incorrectly recorded.

The available research suggests that all of these assumptions may be unsafe. A study undertaken using the Prêt à Voter scheme identified several problems and showed that had difficulties understanding several of the key Prêt à Voter concepts and mechanisms [12]. Voters were unsure why they had to separate the two columns of the ballot paper and destroy the left hand column containing the ordering of candidates. One group in the study failed to destroy it at all, leading to a degraded mode of operation that threatened vote secrecy.

Once they had obtained their receipt many participants were disappointed by the unintuitive nature of it; some expected a document saying who they actually voted for, rather than the weaker guarantees required to maintain receipt-freeness. At the verification stage participants again expressed apathy - some participants opined that current elections run fine without the use of receipts and others felt that the comparison of receipts to bulletin-board values did not provide them with useful information. Storer et al. [13] identified similar limitations in a study of a scheme with significantly simpler verification mechanisms (that was not receipt-free). Additionally, studies of the usability of voter-verifiable voting systems (such as Winckler et al. [14]'s study of Prêt à Voter) suggest that voters considered such methods less usable than paper- or machine-based alternatives.

Voters' uptake of the post-election verification processes tends to be low, such as the 4% recorded during a real-world deployment of Scantegrity [15]. It is currently difficult to quantify what level of uptake is necessarily to obtain reasonable confidence in the accuracy of the result. Risk-limiting audits can provide high confidence with very small samples [16], but this relies on obtaining a random sample of ballots, while the self-selecting sample of verifying voters is likely to be demographically biased.

Separately, the verification elements of the system in the Prêt à Voter study also led the participants to doubt the security of the system. In broad terms they felt that a secure system would not need verification and so conversely the presence of verification must imply a risk of insecurity and consequently be untrustworthy. This perception was also detected during trials for public body elections in the Netherlands [17].

Consequently, this paper argues that existing RFVV schemes do not take adequate account of the socio-technical context in which voting takes place. Specifically, RFVV schemes assume capabilities and motivations on the behalf of voters that are not realistic in a real election context.

RFVV schemes generally ignore the other actors in a voting system and the role that they might play in assuring the correctness of a result. In established democracies, the voting system has evolved in theory and practice to support the role the candidates and other participants play, and practical verifiable voting systems should harness these resources as well.

Political candidates and parties play an important role in the running and auditing of elections. In the United Kingdom, the candidate's appointed counting agents act as scrutineers of election results, alongside election administrators and independent observers [18]. The parties' records from supporters and canvassing can also be used to 'sanity check' the results of the election. This arrangement reflects the very strong incentives for candidates to ensure the correct counting of votes, as this could make the difference between winning and loosing the election. While each individual candidate has no incentive to ensure that votes for other candidates are correctly counted (indeed, they have incentives to encourage the opposite) the candidates as an aggregation have strong incentives to ensure that all votes are correctly counted.

In many countries an important role is also played by Non-Governmental Organisations (NGOs) which aim to promote effective democracy and the fair running of elections. These can include international bodies and observers (e.g. the OCSE), domestic campaign groups (e.g. the Electoral Reform Society in the UK) and civic organisations (e.g. the League of Women Voters). These organisations are non-partisan, and often run campaigns to improve turnout and combat electoral fraud. In less mature democracies the reports of these organisations contribute significantly to the international recognition (or not) of the fairness of the result. It is therefore important that any implementation of RFVV systems provides similar opportunities for external observation and audit as currently used paper-based elections, which has been identified as a difficulty by the Council of Europe [19].

Consequently, this paper proposes that the limitations of voter verification can be mitigated by harnessing the motivation and resources of third-parties to ensure fair elections. The paper is structured as follows. Section 2 examines related work on third-parties in electronic voting and other secure systems. Section 3 outlines a generic adaptation to RFVV schemes that allows the act of election verification to be transferred from voters to third parties without violating voting privacy. Section 4 applies the adaptation to several existing RFVV schemes and analyses the modification for the introduction of vulnerabilities. Section 5 examines different configurations of the generic approach and discusses the viability of several attacks on the generic principle. Section 6 concludes with an overview of the paper and outlines the advantages of this approach.

2. Related Work

Relatively little previous work has considered the role of third-parties in verifiable elections, but some important aspects have been discussed.

In their paper on Scratch & Vote Adida and Rivest [5] suggest a goal of cryptographic voting is to 'trust third parties as little as possible'. However, they also suggest the use of 'helper organisations' including political parties and campaign groups who would provide the equipment necessary for voters to perform their pre-voting validation, presumably via by their presence in the polling station. Similarly, Rivest and Smith [3] sketch out a modified version of their OneBallot system where voters receive the receipts of *previous* voters and suggest the involvement of external organisations to verify the receipts' digital signatures.

The most substantial work on third-party verification is by Neumann et al. [20], who propose the use of third-party websites and mobile apps to verify votes cast using the Helios [21] remote electronic voting system. In this adaptation, respected third-parties provide services by which voters can verify both whether their vote has been correctly constructed and whether it has been correctly stored. This is performed by communicating the voter's witness to a third-party, which then performs the necessary cryptographic checks. User studies using prototype websites suggest a high but not complete rate of success (~80%) in using these verification services. However, this differs from the scheme presented in this paper in a number of important ways:

- Their work applies to remote voting, while our scheme is designed for in-person voting.
- Their scheme reduces the amount of effort required for voters to verify, while ours allows delegate away this effort entirely.
- In their scheme challenges must still be initiated by individual voters, rather than by third-parties.

More generally the use of third-party organisations and systems to address usability issues and improve security can be seen in other domains, such as the increasingly widespread use of password managers. While the introduction of such tools can introduce additional vulnerabilities [22] they can address users' difficulties in managing complex security requirements.

3. Third-Party Verifiability

Figure 1 illustrates the generic arrangement of a receipt-free voter verification scheme. A typical scheme assumes that voting takes place in a secure environment, realised by a polling booth, in which the voter can exchange information with the voting system that cannot be leaked to another actor.

The voter engages in a *cut and choose* protocol [23] with the voting system to prepare a vote and a *witness* for the vote. The witness is a partial, encoded form of the vote - it contains information that can be used to verify that a voter is correctly processed, but cannot be used to determine the voting intent itself. In this approach, the voter is provided with a vote and witness by the system, and can choose whether to cast the vote or immediately audit the witness for correctness. As a result the protocol forces the voting system to decide whether to prepare a valid or corrupt witness before the voter performs any checks, as it not possible to determine whether the witness will be audited or not.

After voting has completed the results and processed by the voting system and made publically available. The voter can then use their witness to confirm that their vote has been counted accurately, but not demonstrate *how* they voted to a third party.

Receipt-free voter-verifiable (RFVV) schemes therefore impose load on the voter at two main points: witness generation and post-election verification. At the witness generation stage some property of the voter's intention is recorded, often in a cryptographic manner. It is critically important that the witness is a well-formatted encoding of that property, but the voter may well not have the understanding or resources needed to check that the witness does indeed match their actual vote. At the verification stage the voter must check that their witness corresponds accurately to a published record, but they may not understand the procedure, and lack incentives to do so.

In both these stages it is possible to replace the voter as the verifying actor and transfer the responsibility to third parties, harnessing their increased incentive and motivation to ensure that votes are correctly formatted and that their presence in the count is verified. The use of pre-filled ballots and secure anonymous channel witness gathering as outlined here is a simple method that can be applied to most existing voter-verifiable voting systems.

During the run-up to the election the ballot is designed in the normal way for the particular voter-verifiable voting system in use. However, no blank ballots are provided to voters: instead, a sufficient quantity of pre-marked ballots for each candidate (more generally, each potential voting option) are produced. These are produced by the authorities and examined by the third party observers (by cut-and-choose or similar method). To preserve receipt-freeness these examined ballots should be discarded, rather than being used. During this process observers ensure that ballot are pre-filled in the correct way, and that the witness (also pre-printed) is correctly structured. This effectively replaces the need for the voter to perform the cut-and-choose protocol, simplifying their voting experience and removing the need for them to understand the underlying cryptographic features. These problems were identified in the use of Scantegrity in Takoma Park [15], where pollworkers suggested that pre-produced receipts would help voter understanding and improve usability.

After the observers are satisfied with their checks, new sets of prepared ballots are then loaded into simple mechanical dispensing machines that are deployed to the polling stations, potentially after a further third-

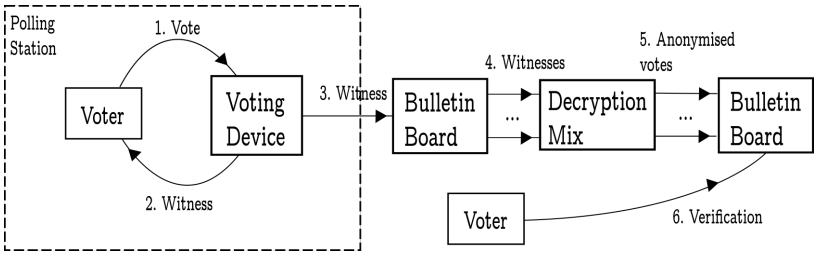

Figure 1: A generic Receipt-Free Voter Verifiable Voting scheme

party check of correctness on these machines. The voter then uses said dispensing machine within the privacy of the polling booth, which issues a pre-filled vote/witness pair for the voter's chosen candidate. The chosen ballot can then be folded over or sealed within an envelope to hide the choice, and then be cast be in the traditional manner. (Variations on the concept of pre-filled ballots are already in use in several democracies, such as the 'ballot letters' in Israel and 'bulletins' of France, and in both cases sealed envelopes are used)

After casting their ballot the voter is then able to deposit their witness securely and anonymously (such as via ballot boxes or more elaborate methods) with the candidate or external organisation of their choice. Depositing their witness with the candidate they voted for harnesses the strongest incentives, but the participation of non-candidate organisations provides freedom of choice to the voter, and reduces the potential leaking of voting intention by implication. Once the result has been declared the candidates and organisations verify the witnesses deposited with them using the standard process for the voting system, and challenge the results if necessary in the usual manner. The overall procedure is highly similar to the RFVV arrangement, and is illustrated in Figure 2.

This approach can be applied effectively to any electoral system where it is possible to refine selections down to a small number of 'tickets' (by political party or otherwise), due to the need to limit the number of different pre-filled ballot permutations. This includes simple majoritarian (first-past-the-post) elections and referendums as well as proportional representation or mixed-member systems that use closed party lists. Additionally, it is broadly compatible with systems that require exhaustive preferences where parties publish guides to their voters describing the parties' ideal set of preferences, such as in Australian Senate elections. This approach is unlikely to be suitable for elections using preferential voting or elections featuring large numbers of distinct candidates, as the number of ballot permutations becomes intractable.

4. Applications

The use of pre-filled ballots allows voter-verifiable voting systems to be easily converted into third-party verifiable voting systems, while allowing the same procedures to be used and the same security properties obtained as in the original, unmodified system. This section of the paper examines adapted versions of Scantegrity and Prêt à Voter . In each case a brief outline of the original system is provided, followed by details of the adaptations made. In particular, risks and attack vectors introduced or removed by the modifications are examined.

4.1. Scantegrity

Scantegrity is a witness-based voter-verifiable voting system that is widely studied, and one of the few to be used for binding political elections [1]. The Scantegrity ballot takes the form of a standard machine readable bubble ballot, with two important additions. Cryptographically generated code letters are placed beside the name of each candidate, and a unique serial number is printed in both human and machine readable forms. After voting, the voter separates off part of the ballot containing a copy of the serial number,

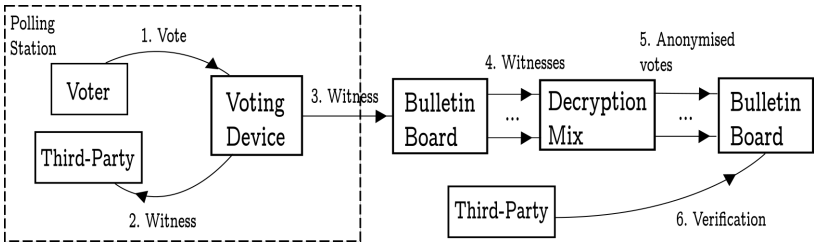

Figure 2: Conceptual model of third-party verifiability

and they should also record the code letters for their chosen candidate. After counting the serial numbers and code letters for the selected candidate are published. The voter can then check that their own record of the code letters matches the published version. If they do not match the voter can challenge the result, but the dispute resolution process is fairly unintuitive, although later versions of Scantegrity offer some improvements.

The pre-filling process is straightforward at the ballot preparation stage, but can be used to later simplify the dispute resolution process. The appropriate code letters can be pre-printed onto the witness portion of the ballot, and secured by the use of watermarks or similar security techniques. As a result the complex process necessary to protect against malicious disputes can be eliminated, making verification much more streamlined. Malicious election authorities might attempt to deliberately print the wrong code letters on the witness to cast doubt on the accuracy of the election, but as this can be detected by a visual check the practicality of this attack is limited.

The voter's experience is simple, as they merely have to select the candidate of their choice and check that the correct candidate is marked on the dispensed ballot. The ballot and witness can be issued on the same piece of paper (as in classic Scantegrity), or they can be pre-separated, ensuring that the two parts are distinguishable and that the voter does not leave the witness attached when casting their ballot.

After casting the vote witnesses are deposited with the voter's choice of candidate or observer via a secure and anonymous system. At the close of polls the serial numbers and code letters are published to a bulletin-board as standard, and those in possession of the ballots can check that all their witnesses appear correctly in the published list. If there is discrepancy they can challenge the election authorities using their witness. The use of pre-filled, watermarked witnesses means that the challenger has strong evidence that their witness is authentic so changes to the record and investigations into the cause of the discrepancy can begin without the need to perform a lengthy procedure to test the validity of the witness.

4.2. Prêt à Voter

Prêt à Voter was one of the first voter-verifiable voting systems using a similar ballot layout to conventional paper voting [8]. The Prêt à Voter ballot consists of two columns - the left column contains the list of candidates (in alphabetical order with a random offset) and the right column contains spaces for marking the vote as well as an alphanumeric value known the onion. The onion is a representation of the candidate ordering that has been public key encrypted by a sequence of tellers. The voter marks the right column alongside the appropriate candidate, then separates and destroys the left column. This leaves only the right column, which merely has one marked section and the onion. This column is fed into an optical scanner within the polling booth, which records this information and transfers it to the central election server and then returns the column. At the close of polls the tellers acting together can decode the onion to reveal the ordering and hence work out which candidate was voted for. The voter is then able to check that their vote (identifiable by the onion value) has been included in the count, and that their mark is recorded in the correct section.

At ballot production pre-filled Prêt à Voter requires minimal modifications. The appropriate section of the right-hand column is marked. When voting the voter simply need check the correct candidate is marked. One common problem encountered during the Prêt à Voter focus groups was that voters did not understand the importance of separating the two columns, and so there is an argument for providing the two elements to the voter separately in the first place, or even not providing the left column at all. However, the voter cannot check the correctness of their vote from the right column alone and so maintaining the standard layout is important to improve voter confidence. Instead the voter could be issued with two ballots each containing both columns, with one marked ballot and one marked witness. The separation of the columns is normally used to provide coercion resistance for the voter, but this is unnecessary in a compulsory deposit system, as the voter never leaves the polling station with the witness, which is instead anonymously deposited, breaking the link to the individual voter and the possibility of coercion.

Having cast their ballot and deposited their witness the voter's role is complete, and the election results are produced and the witnesses are published to a bulletin-board. The candidates and observers check for the presence and correctness of the witnesses they hold and can challenge the results if necessary using the standard Prêt à Voter procedure.

5. Discussion

The general approach outlined earlier presents one possible configuration of a third party-verifiable voting system. Different configurations are possible using the same principles; different configurations offer a subtly different balance of strengths and weaknesses and may be more suitable in particular contexts and applications. There are three main sections that can be configured differently - ballot creation, ballot depositing and compulsion of deposit.

Additionally, the move to a third-party verifiable voting system changes the security properties of a voting system. The advantages of such an approach have already been outlined, but changes to security assumptions and new potential attacks are discussed below.

5.1. Ballot Creation

Pre-marked ballot papers must be prepared in sufficient quantities prior to the opening of the polls. These should be produced and marked by the election authorities, with the third-party observers auditing a proportion. This approach most closely matches current electoral procedures, and offers efficiencies of scale in production. The exact details of the pre-marking should be agreed in advance to provide confidence in their accuracy, and observers should be able to cut-and-choose which ballots they wish to inspect. In this approach the primary risk comes from the election authorities attempting to discriminate against certain candidates by malforming their ballot or manipulating the witness element. Candidates without sufficient resources may not be able to check enough ballots to detect subtle attacks, so the participation of other third parties to check these ballots provides additional safeguards.

5.2. Witness Depositing Mechanisms

The depositing of witnesses is required to transfer the information encoded in the witness from the voter to a third party. This process needs to be secure and offer one-way anonymity (the party receiving the receipt should not be able to identify which voter it came from). Additionally, it is preferable that the voter's choice of third party should be private so that inferences on voting intention cannot be drawn.

The simplest way to implement this process is to provide a selection of additional ballot boxes in each polling station, with each third party assigned their own box. While straightforward, this approach does not provide any privacy for the voter, and so those within the polling station may be able to guess at their voting intention based on their choice of third party. To obtain voter privacy while maintaining the public aspect of the ballot box (which acts as a protection against stuffing and removal of receipts) a mechanical box could be constructed that enables the voter to choose between third parties using a switch or dial. The public nature of the box itself is preserved, but the voter's choice of third party is kept

private. This approach offers good privacy, but may not be easy to construct or maintain, and risks voters making the wrong selection or not understanding the system. A comprise between usability and privacy can be obtained by using an optical scanner to record the witness, details of which can be transferred electronically to the third party. This type of device is already in wide use for recording ballots, and can be programmed to provide a rich user interface. DRE systems can be attacked to leak information or discard ballots, but the consequences of such attacks are less severe when scanning witnesses than when scanning actual votes.

5.3. Compulsory Depositing

Third-party verifiable systems move the primary responsibility for witness verification from voters to candidates and external observers. This move can be either partial or complete; voters may or may not still have the option to verify their vote themselves. Compulsory deposit schemes offer a number of advantages over partial depositing. If witnesses are not removed from the secure environment of the polling station it becomes possible to include more information on them without endangering security or privacy; witnesses in a partial depositing system must stop the voter from revealing their choice of vote, but this necessity is eliminated if the witness does not leave the polling station.

Witnesses are instead only required to be anonymous when deposited, enabling considerably simpler methods of vote challenging to be enabled by encoding more information in the witness. The voting experience is made simpler, as the voter is not required to consider the possibility of verifying their vote themselves. This approach may also increase the proportion of votes verified, if candidates and observers can be assumed to verify all or the large majority of votes deposited with them. This approach necessarily assumes that the removal of witnesses from the polling station can be prevented, akin to the existing practices for deterring chain voting.

However, the compulsory deposit scheme does not provide any option for the voter who distrusts both the election authorities and all avaliable third parties, as they are unable to verify the correctness of the election independently.

5.4. Security Assumptions

The security and privacy properties of receipt-free verifiable voting systems are subject to a set of assumptions, which vary according to the particular structure and design of each system. These assumptions may include the behaviour of the voters or the election authorities (such as assuming a certain threshold of authorities are trustworthy) as well as assumptions about the technical factors in the system design (such that certain cryptographic operations cannot be effectively reversed).

In general, a third-party verifiable modification to an existing voter-verifiable voting system should require only a minimal set of additional security assumptions on top of those in the original system. As in a voter-verifiable system, the detection of electoral manipulation requires that a suitable proportion (that is both large and random enough) of verifiers actually perform verification; accuracy of the result cannot be assured if third-parties are lax in their verification. The receipt-freeness of the election (and the inability of the voter to prove their vote, even if they wish to) is guaranteed by the existing voting system design (and subject to the assumptions therein) assuming the existence of a truly anonymous channel for witness deposit.

Some specific variants of third-party verification also rely on additional assumptions. Compulsory depositing relies on the assumption that either the electoral authorities or a suitable well-resourced and independent third party can be trusted; if this assumption is false (such as in an authoritarian one-party state) then manipulation cannot be detected. Additionally, it assumed that witnesses can be prevented from leaving the polling station. Similarly, the creation of pre-marked ballots assumes a trustworthy authority or at least one independent observer.

5.5. Potential Attacks

The use of pre-filled ballots means that significantly more ballots are produced, and that all these ballots are potentially valid votes. This places additional

emphasis on the need for strong chains of custody and rigorous polling station procedures. If a proportion of the uncast pre-filled ballots were obtained by an attacker they could be used for a ballot stuffing attack, which would be easy to detect but difficult to correct. Additionally, an attacker obtaining pre-filled ballots could separate off the witness elements, and pass them on to one of the candidates. This candidate could them claim that these votes had been ignored by the election authorities, and use the witness as proof of this. This type of attack can only be addressed if comprehensive records of the issued ballots are kept.

By moving the process of ballot verification (e.g. by 'cut and choose') to before the opening of polls, this approach may make it easier for malicious election authorities to manipulate ballots. Good physical security should prevent the authorities from modifying existing ballots or inserting additions between the verification phase and the actual dispensing to the voters, but it is easier to mount an attack when the process of verification is planned in advance. This can be addressed by allowing third parties to randomly inspect the stockpiles of ballots and dispensers at polling stations during the voting period, enabling them to detect modifications if they lack trust in the physical security of the election.

The use of a dispensing machine provides a point of attack, although this device is less vulnerable than electronic voting devices. The machine may be manipulated to dispense the wrong ballot for particular candidates, but this attack can be easily detected by the voter when they see that another candidate is marked on their ballot paper (this attack becomes more effective if used against a voting system with complex ballots that the voter may not understand, such as ThreeBallot). In theory ballot stuffing could be encouraged by the ability to obtain multiple ballots from the dispenser; this can be alleviated by enforcing a timeout between the dispensing of ballots, akin to the delay on Indian EVMs. The device could be bugged in order to obtain partial information as the election is ongoing, but the same level of information could be leaked in any system that uses a polling station based ballot scanner.

The distribution of witnesses to (multiple) third parties provides these entities with potentially significant partial information about ongoing voting. The strength of this information is related to the properties of the witness; in classic Scantegrity and Prêt à Voter it is not possible to determine the voter's choice from the witness (receipt-freeness), although this would be possible in the modified version of Prêt à Voter suggested above. However, the simple act of depositing a witness with a third-party provides that third-party with information about the number of votes cast and the likely voter turnout. However, there are two main reasons that this partial information is of limited use to a malicious third-party. Firstly, the proportion of voters who deposit their witnesses with any specific third-party is unpredictable and usually (depending on the physical layout and security of the polling station) unmeasurable while the vote is ongoing. As a result, it is not practical to extrapolate wider predictions from a set of deposited ballots. Secondly, ongoing turnout information is often published by election authorities at certain intervals; the only advantage from witness-derived information would be if it was obtainable at a more granular level than official announcements.

A number of practical attacks have already been documented on the Scantegrity and Prêt à Voter systems, and these are not discussed here unless the modification particularly enhances or diminishes their threat.

6. Conclusion

Voter-verifiable voting systems place significant demands on the voter during ballot completion, witness comparison and post-election verification. If voters do not complete or understand these processes the benefits of the systems can be lost, and additional problems introduced in terms of system usability and security. Unfortunately voters lack incentives to participate fully and knowledgeably in such systems, and evaluation evidence shows a significant lack of understanding and deviation from required procedure.

In contrast candidates and third-party observers have the incentives and motivation to verify that votes cast actually counted, and hence have the desire and resources to perform effective, large-scale verification. A generic system of pre-filled ballots has been outlined

that allows ballot completion and witness comparison to be performed in advance of the vote by the candidates and election authorities. Combined with the use of a secure polling station depositing system allowing transfer of the witnesses to third-parties this generic approach eliminates the main areas of cognitive load from the voter's experience, while maintaining the security properties and audibility advantages of voter-verifiable systems. Applying this approach to two major voter-verifiable voting systems shows that only simple changes are needed to apply it in practice and in some cases it can provide additional benefits in addition to those obtained from the move away from voter-verification.

References

[1] D. Chaum, A. Essex, R. Carback, Scantegrity: End-to-end voter-verifiable optical-scan voting, in: IEEE Security & Privacy, 2008.

[2] D. Chaum, R. Carback, J. Clark, A. Essex, Scantegrity II: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes, in: USENIX Electronic Voting Technology Workshop, 2008.

[3] R. L. Rivest, W. D. Smith, Three Voting Protocols: ThreeBallot, VAV, and Twin, in: EVT'07 Electronic Voting Technology Workshop, USENIX/ACCURATE, Boston, MA, 2007.

[4] B. Adida, Advances in Cryptographic Voting Systems, Ph.D. thesis, Massachusetts Institute of Technology, 2006.

[5] B. Adida, R. Rivest, Scratch & Vote, Proceedings of the 5th ACM Workshop on Privacy in Electronic Society (2006) 29–39.

[6] D. Chaum, Secret-Ballot Receipts: True Voter-Verifiable Elections, IEEE Security and Privacy 2 (1) (2004) 38–47.

[7] P. Y. Ryan, Prêt à Voter With a Human-Readable, Paper Audit Trail, in: Frontiers of Electronic Voting, Schloss Dagstuhl, Germany, 2007.

[8] D. Chaum, P. Ryan, S. Schneider, A practical voter-verifiable election scheme, in: Computer SecurityâĂŞESORICS 2005, 118–139, 2005.

[9] B. Randell, P. Y. Ryan, Voting Technologies and Trust, Tech. Rep. CS-TR-911, School of Computing Science, University of Newcastle, 2005.

[10] D. J. Reynolds, A Method for Electronic Voting with Coercion-Free Receipt, in: Frontiers in Electronic Elections (FEE 2005), Milan, Italy, 2005.

[11] NIST, Draft Standard for Voter Verified Paper Audit Trails in DRE Voting Systems (DRE-VVPAT): Supplement to the 2002 Voting Systems Standard, National Institute of Standards and Technology (NIST), draft edn., 2005.

[12] S. Schneider, M. Llewellyn, Focus group views on Pret a Voter 1.0, Requirements Engineering for Electronic Voting (2011) 56–65.

[13] T. Storer, L. Little, I. Duncan, An exploratory study of voter attitudes towards a pollsterless remote voting system, in: Workshop on Trustworthy Elections, 2006.

[14] M. Winckler, R. Bernhaupt, P. Palanque, D. Lundin, K. Leach, P. Ryan, E. Alberdi, L. Strigini, Assessing the usability of open verifiable e-voting systems: a trial with the system Prêt à Voter, in: Proc. of ICE-GOV, 2009.

[15] R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. Herrnson, T. Mayberry, S. Popoveniuc, R. Rivest, E. Shen, A. Sherman, P. L. Vora, Scantegrity II municipal election at Takoma Park: the first E2E binding governmental election with ballot privacy, in: USENIX Security, 2010.

[16] M. Lindeman, P. Stark, V. Yates, BRAVO: Ballotpolling Risk-Limiting Audits to Verify Outcomes, 2012 Electronic Voting Technology Workshop (i).

[17] W. Pieters, Verifiability of Electronic Voting: Between Confidence and Trust, Data Protection in a Profiled World (2010) 157–175.

[18] R. Blackburn, The Electoral System in Britain, St. Martin's Press, 175 Fifth Avenue, New York N.Y. 10010, 1995.

[19] Directorate General of Democracy and Political Affairs, Workshop on the observation of e-enabled elections, Tech. Rep. March, Council of Europe, 2010.

[20] S. Neumann, M. M. Olembo, K. Renaud, M. Volkamer, Helios verification: To alleviate, or to nominate: Is that the question, or shall we have both?, in: Proceedings of the International Conference on Electronic Government and the Information Systems Perspective, ISBN 9783319101774, 2014.

[21] B. Adida, Helios: Web-based Open-Audit Voting., in: Proceedings of the 17th USENIX Security Symposium, 335–348, 2008.

[22] Z. Li, W. He, D. Akhawe, D. Song, The Emperor's New Password Manager: Security Analysis of Web-based Password Managers, in: Proceedings of the 23rd USENIX Security Symposium, ISBN 978-1-931971-15-7, 2014.

[23] B. Schneier, Applied Cryptography, John Wiley & Sons, 605 Third Avenue, New York, N.Y. 10158-0012, third edn., ISBN 0-471-11709-9, 1996.